

CORPORATE CONTINGENCY PLANNING WORKPROGRAM

CHAPTER 10WP

(FILE NAME ON DISK #3= IS-WP#05.WPD)

COMMENTS

This section is intended to determine whether senior management has instituted a current and workable corporate contingency planning process throughout the organization. Management must develop and maintain an effective recovery planning process in the event a disaster or major disruption disables any functional area(s) of the institution or any of the IS supporting infrastructure that service(s) them. An organization-wide focus to recover must be developed for all IS areas from the smallest stand-alone PCs and LANs to centrally located minicomputers or the central mainframe computer center. All IS support activity and the functional customer areas they serve must have a clearly defined and fully integrated recovery plan. The direction for such planning must originate from the senior level and address fully all aspects of the institution's operational activity that supports the delivery of services to both internal and external customers. The examiner should document findings, especially those that do not satisfy the recommendations outlined in the 1996 *FFIEC IS Examination Handbook*. This document will be included in the workpapers.

CORPORATE CONTINGENCY PLANNING

1. Determine if the board has approved an organization-wide contingency plan within the last 12 months.
2. Determine if a senior manager has been assigned responsibility to oversee the development, implementation, and maintenance of the corporate contingency plan.
3. Determine if management periodically reviews and prioritizes each business unit, department, and functional unit for its critical importance. If so, determine how often are reviews conducted.
4. Review the written corporate contingency plan and verify if the plan:
 - a. Addresses all the critical business units/departments/functions identified in step 3.
 - b. Has a clear and current employee/manager notification tree.
 - c. Clearly defines responsibilities and decision-making authorities for designated teams and/or staff members.
 - d. Documents guidelines for recovery-related expenses for later insurance or tax-loss claims.

- e. Designates a public relations spokesperson.
 - f. Identifies sources of needed office supplies and equipment.
 - g. Addresses the recovery of free standing PCs and LANs. If this is not included in the plan, check to see there is a separate plan for recovery of these resources.
- 5. Determine if adequate procedures are in place to ensure the plan is maintained in a current fashion and updated regularly.
 - 6. Determine if personnel are adequately trained as to their specific responsibilities under the plan.

TESTING

- 7. Check to see how often is the corporate contingency plan tested.
- 8. Verify that all critical business units/departments/functions are included in the testing.
- 9. Verify that tests include:
 - a. Setting goals in advance.
 - b. Realistic conditions and activity volumes.
 - c. Use of actual backup system and data files from off-site storage
 - d. Participation and review by internal audit.
 - e. A post-test analysis report and review process that includes a comparison of test results to the original goals.
 - f. Development of a corrective action plan for all problems encountered.
- 10. Determine if interdependent departments have been involved in testing at the same time to uncover potential conflicts.

IS CONTINGENCY PLANNING

- 11. Determine if the data center has a properly documented contingency plan. Verify that the IS

contingency plan properly supports and reasonably reflects the goals and priorities found in the corporate contingency plan.

12. Review the written IS contingency plan to determine if it:
 - a. Clearly identifies the management individual(s) who have authority to declare a disaster.
 - b. Clearly defines responsibilities for designated teams or staff members.
 - c. Explains actions to be taken in specific emergency situations.
 - d. Allows for remote storage of emergency procedures manuals.
 - e. Defines the conditions under which the backup site would be used.
 - f. Has procedures in place for notifying the backup site.
 - g. Has procedures for notifying employees.
 - h. Establishes processing priorities to be followed.
 - i. Provides for reserve supplies.
13. Determine if all critical resources are covered by the plan, including data communication networks, ATMs, etc.
14. Determine if the plan includes stand alone PCs and LANs. If it does not, check to see if there is a separate plan for those resources.
15. Determine if a copy of the IS contingency plan is stored offsite.

HARDWARE BACKUP

16. Describe arrangements for alternative processing capability in the event the data center or any portion

of the work environment becomes disabled and document that the arrangements are in writing.

17. If the organization is relying on in-house systems in separate physical locations for backup, verify that the equipment is capable of independently processing critical applications.
18. If the organization is relying on outside facilities for backup, determine if the backup site:
 - a. Has the ability to process the required volume.
 - b. Provides sufficient processing time for the anticipated workload based on emergency priorities.
 - c. Allows the institution to use the facility until it achieves a full recovery from the disaster and resumption of activity at the entity's own facilities.
19. Determine how customers would be accommodated if simultaneous disaster conditions were to occur to several customers of the backup facility provider.
20. Determine whether the institution would be kept informed of any changes at the recovery site (e.g. hardware or software upgrades or modifications) that might require adjustments to the institution's software or to the recovery plan.
21. Determine if the plan provides physical security at the recovery site.

PROGRAM OR SOFTWARE RECOVERY

22. Coordinate with the review of backup tape creation and rotation procedures performed under the operations workprogram and determine if:
 - a. Duplicates of the operating system are available both on- and off-site.
 - b. Duplicates of the production programs are available both on and off-site. Including both source and object versions.
 - c. All programming and system software changes are included in the backup.

- d. Backup media is stored off-site from which it can be retrieved quickly at any time.
- 23. Review the written IS contingency plan and determine if the plan addresses the backup of the systems and programming function (if applicable), including:
 - a. Qualified personnel.
 - b. Backup of programming tools and software.
 - c. Off-site copies of program and system documentation.
- 24. Verify the IS contingency plan provides for logical security procedures at the recovery site.

DATA RECOVERY

- 25. Coordinate with the review of backup tape creation and rotation procedures performed under the operations workprogram and determine if all master files and transaction files are backed up adequately to facilitate recovery should a disaster occur.

NETWORK RECOVERY

- 26. Determine if management assesses the network environment including:
 - a. The individual components in the network.
 - b. The dependence on each component.
 - c. The probability of a component going down or becoming unavailable or unreliable.

TESTING

- 27. Determine if the IS contingency plan is tested at least annually.
- 28. Determine if all critical applications and services tested.
- 29. Determine if the tests include:
 - a. Setting goals in advance.
 - b. Realistic conditions and activity volumes.

- c. Use of actual backup system and data files from offsite storage.
 - d. Participation and review by internal audit.
 - e. A post-test analysis report and review process that includes a comparison of test results to the original goals.
 - f. Development of a corrective action plan for all problems encountered.
30. Determine if several user departments have been involved in testing at the same time to uncover potential conflicts.

CONCLUSIONS

31. Review the results of work performed in this section and in sections for planning, auditing , and management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections.
32. Discuss with management:
- a. Violations of law, rulings, regulations or significant internal control deficiencies.
 - b. Recommended corrective action for deficiencies cited.
 - c. Management's proposed actions for correcting deficiencies.
33. Assign a rating (see Chapter 5 for additional information).
34. Prepare an index of workpapers for this section of the workprogram.
35. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem or high risk areas. Also include, important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the

overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

36. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

Reviewer's Initials